UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Samuel Cox, Sean DeMarco, Nicole Greer, Thomas Leffler, and Jason Yoder, individually and on behalf of all others similarly situated, Plaintiffs, v. Capital One Financial Corporation, Defendant.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Samuel Cox, Sean DeMarco, Nicole Greer, Thomas Leffler, and Jason Yoder ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, bring this Class Action Complaint against Capital One Financial Corporation ("Capital One").

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Capital One for its failures to employ reasonable and appropriate measures to protect and secure the private, sensitive, and valuable information of Plaintiffs and other Capital One credit card applicants and card holders, which led to and facilitated one of the largest data breaches to a U.S. financial institution in history.

2. On July 19, 2019, Capital One determined that on March 22–23, 2019, an outside individual gained unauthorized access (the "Data Breach") to electronic financial records relating to approximately 100 million of Capital One's customers and credit card applicants from 2005

through early 2019, which included one or more of the following data fields: names, addresses, zip codes, phone numbers, e-mail addresses, dates of birth, Social Security numbers, bank account information, income, credit scores, credit limits, credit card balances, credit card payment history, and transaction data (the "Financial Records").

3. Capital One announced the Data Breach on July 31, 2019, via press release. In the press release, Capital One said it would notify approximately 120,000–200,000 of the affected individuals, but not the other approximately 99.8 million affected U.S. individuals who had their highly sensitive and valuable Financial Records compromised in the Data Breach.

4. Due to Capital One's deficient and unreasonable security, Plaintiffs' and Class members' Financial Records were accessed, copied, decrypted (to the extent the data was ever encrypted), and stolen by at least one hacker with a demonstrated intent to distribute the information further. Using well-known methods, the hacker exploited "immediately fix[able]" vulnerabilities in Capital One's systems and made away with 100 million Financial Records undetected. The only reason Capital One ever learned of the Data Breach was because the hacker we know about, who has since been apprehended and indicted, told an anonymous third party about the stolen Financial Records and the third party notified Capital One.

5. Capital One's deficient and unreasonable security enabled and facilitated the unauthorized access and acquisition of Plaintiffs' and the other Class members' Financial Records. Capital One's deficient and unreasonable monitoring of its systems enabled and facilitated the severe magnitude and duration of the Data Breach.

6. Capital One's conduct has injured and will continue to injure Plaintiffs and the other Class members and put them at serious, immediate, and ongoing risk of identity theft, fraud, and

will cause costs and expenses in responding, identifying, and correcting damages that are reasonably foreseeable as a result of Capital One's wrongful conduct.

7. Accordingly, Plaintiffs, on behalf of themselves and all others similarly situated, assert claims for negligence, negligence per se, breach of confidentiality, statutory causes of action under the laws of states where they reside, and unjust enrichment. Plaintiffs seek monetary damages, punitive damages, statutory damages, and injunctive and equitable relief, and all other relief authorized in law and equity.

JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because there are 100 or more Class members, at least one Class member is a citizen of state that is diverse from Defendant's citizenship, and the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

9. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to these claims occurred in this District.

PARTIES

10. Plaintiff Sean DeMarco is a citizen of California. In April 2015, he applied for a Capital One Quicksilver card. In May 2015, he applied for a Capital One Venture card. At the time of the Data Breach he was a cardholder.

11. Plaintiff Samuel Cox is a citizen of Florida. In 2018, he applied for a Capital One Bass Pro Club Credit Card and at the time of the Data Breach was a card holder.

12. Plaintiff Jason Yoder is a citizen of Tennessee. He applied for a Capital One credit card in 2014 or 2015 and at the time of the Data Breach was a card holder.

13. Plaintiff Nicole Greer is a citizen of Tennessee. She applied for a Capital One card in or around 2009 and at the time of the Data Breach was a card holder.

14. Plaintiff Thomas Leffler is a citizen of Wisconsin. He applied for a Capital One credit card in 2009 and another one in 2012, was approved both times, and at the time of the Data Breach was a card holder of a Capital One Venture card.

15. Defendant Capital One Financial Corporation is a Delaware corporation with its principal place of business in Virginia. Capital One is one of the largest credit card issuers in the nation.

FACTUAL BACKGROUND

The Data Breach

16. At least from March 22–23, 2019, an unauthorized outside person gained access to confidential and sensitive Financial Records gathered and maintained by Capital One, exploiting a well-known type of vulnerability in place in Capital One's information system using a method known as "Server Side Request Forgery."

17. In Capital One's own words, the vulnerability was "immediately fix[able]."

18. The unauthorized outside person identified a misconfiguration in the Web Application Firewall (WAF) that allowed intruders to trick the firewall into relaying requests to internal systems and pulled Capital One access credentials, which were then used to access, request, download, and steal the Financial Records. The methods deployed by the hacker have been well understood and warned about by cybersecurity specialists since before the Data Breach.

19. Capital One failed to detect or prevent the unauthorized access and acquisition of the Financial Records on approximately 100 million Americans and failed to notice it for nearly

four months, even though the hacker was communicating about the Data Breach to others online and through social media.

20. Finally, on July 17, 2019, an anonymous individual who was contacted by the hacker notified Capital One via email that a leaked file containing the Financial Records was on GitHub, a website where software developers collaborate. It took Capital One an additional two days, and on July 19, 2019, Capital One discovered the Data Breach.

21. According to Capital One, the data the hacker was able to access, retrieve, and steal information primarily related to credit card applications. On July 29, 2019, Capital One announced that "unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers."

22. Capital One has stated that the stolen Financial Records contain sensitive personal and financial information including, but not limited to:

- names
- addresses
- zip codes
- phone numbers
- e-mail addresses
- dates of birth
- income
- credit scores
- credit limits
- balances
- payment history
- contact information
- 23 days' worth of transaction data

- 140,000 Social Security numbers
- 80,000 linked bank account numbers

23. Capital One will "directly notify" only the persons who had their Social Security and bank account numbers exposed, but will not directly notify any of the nearly 100 million Americans who have been injured and endangered by the Data Breach.

24. The Financial Records relate to credit card applications submitted to Capital One as early as 2005. Capital One has thus placed a significant onus on Plaintiffs and the other Class members to ascertain whether they are Class members and what information of theirs was subject to the Data Breach and is now exposed to identity theft, fraud, and misuse.

25. Even though Capital One states that it "immediately fixed" the security vulnerability that was exploited by the hacker, it actually took months for it to become aware that 100 million records were vulnerable, accessible, and in the hands of unauthorized persons. Capital One did not even know the hacker was touting the Data Breach on social media, even providing details about the method of carrying it out. Furthermore, Capital One was not even the one who discovered the Data Breach, and may never have learned about the breach had a conscientious individual not alerted Capital One and directed it to the compromised Financial Records.

26. Although Capital One's CEO has apologized, Capital One attempts to deny the harm its breach caused and will continue to cause, and in its own self-interest, attempts to deflect responsibility. Capital One publicizes its "analysis" of the breach and asserts, without support and contrary to publicly available evidence, that it is unlikely that the stolen Financial Records were used for fraud or disseminated. Plaintiffs contest that unsupported and self-serving assertion and maintain that they are entitled to all of the evidence and facts on which such "analysis" is based or purportedly based and all evidence and facts in Capital One's possession, custody, or control that

bears on the analysis and investigation. Capital One has placed its forensic reports, investigations, and analysis into the breach into issue.

27. More than a month prior to Capital One's discovery of the Data Breach, the hacker was communicating an intent to distribute the Financial Records. According to a screenshot that Capital One provided to government authorities, on June 18, 2019, the hacker sent a message to the individual who notified Capital One of the breach stating: "Ive basically strapped myself with a bomb vest, [expletive] dropping capitol ones dox and admitting it. I wanna distribute those buckets I think first." Two minutes later the hacker stated: "There ssns…with full name and dob."

28. Brian Krebs, cybersecurity expert and journalist, states that "it seems likely that at least some of that data [the Financial Records] could have been obtained by others who may have followed [the hackers'] activities on different social media platforms."[1]

29. In fact, as one of the foremost repositories of collaborative software development projects, GitHub is a ripe target for attackers to scan and find exposed sensitive information. Numerous data breaches and leaks have occurred on GitHub, including information of Uber, AWS, and Slack. Given the length of time the Data Breach went unnoticed by Capital One and the rampant targeting of GitHub by unscrupulous actors, it is likely that the Financial Records were noticed, accessed, and stolen further.

[1] Brian Krebs, *Capital One Data Theft Impacts 106M People*, Krebson Security, https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/ (last visited Aug. 5, 2019).

Security Breaches Lead to Identity Theft

30. According to The Harris Poll, an estimated 15 million people were victims of one or more incidents of identity theft in 2017. Javelin Research estimates that 16.7 million individuals were impacted by identity theft during the same period.[2]

31. The Federal Trade Commission ("FTC") has cautioned that identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[3]

32. Personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[4] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

---

[2] *See How Common Is Identity Theft? (Updated 2018) The Latest Stats*, LifeLock, https://www.lifelock.com/learn-identity-theft-resources-how-common-is-identity-theft.html (last visited Aug. 2, 2019).

[3] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[4] Companies, in fact, also recognize Private Information as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PERSONAL INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

33. In fact, "[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud."[5]

The Monetary Value of Privacy Protections and Private Information

34. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[6]

35. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[7]

36. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[8]

---

[5] *One in Four that Receive Data Breach Letters Affected By Identity Theft*, Kaspersky Daily, http://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/ (last visited Aug. 2, 2019).

[6] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, Federal Trade Commission, https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited Aug. 2, 2019).

[7] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Aug. 2, 2019).

[8] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Aug. 2, 2019).

37. Recognizing the high value that consumers place on their personal information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their personally identifiable information.[9] This business has created a new market for the sale and purchase of this valuable data.[10]

38. Consumers place a high value not only on their personal information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[11]

39. The value of Plaintiffs' and Class members' Financial on the black market is substantial. Capital One has deprived Plaintiffs and Class members of the substantial value of their information.

Damages Sustained by Plaintiffs and the Other Class Members

40. Plaintiffs and other members of the Class have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Financial Records, which was placed in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) deprivation of

[9] Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited Aug. 2, 2019).

[10] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Aug. 2, 2019).

[11] *See* Erika Harrell, *Victims of Identity Theft, 2014*, U.S. Department of Justice, https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 2, 2019).

the value of their Financial Records, for which there is a well-established national and international market—for which they are entitled to compensation.

41. Plaintiffs and the other Class members have suffered and will continue to suffer additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend and must expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

42. Acknowledging the damage to Plaintiffs and Class members, Capital One is encouraging customers to enroll in account alerts, monitor their credit card accounts, and warning customers to be wary of phishing or scams.

CLASS ACTION ALLEGATIONS

43. Plaintiffs bring this case on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class (the "Nationwide Class") defined as:

> All persons whose Financial Records were affected by the Data Breach.

Excluded from the Class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

44. Plaintiff DeMarco brings this case on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class (the "California Class") defined as:

> All persons residing California during the Data Breach whose Financial Records were affected by the Data Breach.

Excluded from this class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

45. Plaintiff Cox bring this case on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class (the "Florida Class") defined as:

> All persons residing in Florida during the Data Breach whose Financial Records were affected by the Data Breach.

Excluded from this class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

46. Plaintiffs Greer and Yoder bring this case on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class (the "Tennessee Class") defined as:

> All persons residing in Tennessee during the Data Breach whose Financial Records were affected by the Data Breach.

Excluded from this class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

47. Plaintiff Leffler brings this case on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class (the "Wisconsin Class") defined as:

> All persons residing in Wisconsin during the Data Breach whose Financial Records were affected by the Data Breach.

Excluded from this class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

48. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

49. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number approximately one hundred million. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from Capital One's records. Class members may be notified of the pendency of this action by mail, e-mail, Internet postings, or publication.

50. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Capital One failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class members' Financial Records;

b. Whether Capital One properly implemented its purported security measures to protect Plaintiffs' and Class members' Financial Records from unauthorized capture, dissemination, and misuse;

c. Whether Capital One took reasonable measures to determine the extent of the Data Breach after it first learned of same;

d. Whether Capital One willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Financial Records;

e. Whether Capital One was negligent in failing to properly secure and protect Plaintiffs' and Class members' Financial Records;

f. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

51. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other Class members. Similar or identical common law and statutory violations, business practices, and injuries are involved. Individual questions, if any, are predominated, in both quality and quantity, by the numerous common questions that dominate this action.

52. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Capital One's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses that are unique to any Plaintiff.

53. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

54. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are

relatively small compared to the burden and expense that would be required to individually litigate their claims against Capital One, so it would be impracticable for Class members to individually seek redress for Capital One's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS

COUNT I
Negligence
(Brought by All Plaintiffs on Behalf of the Nationwide Class)

55. Plaintiffs incorporate paragraphs 1–54 as if fully set forth herein.

56. Capital One owed numerous duties to Plaintiffs and the other members of the Class. These duties include the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Financial Records in its possession;

b. to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of private, non-public personal information and Financial Records).

c. to protect Financial Records in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

d. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and the other members of the Class of a Data Breach.

57. Capital One knew or should have known the risks of collecting and storing Financial Records and the importance of maintaining secure systems. Capital One knew of the many breaches that targeted other entities in the years preceding the Capital One Breach.

58. Given the nature of Capital One's business, the sensitivity and value of the information it aggregates and evaluates, and the resources at its disposal, Capital One should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, should have detected it earlier than it did, and should never have had such vast quantities of financial information so easily stolen from one location.

59. Capital One knew or should have known that its systems did not adequately safeguard Plaintiffs' and the other Class members' Financial Records.

60. Capital One breached the duties it owed to Plaintiffs and Class members in several ways, including:

a. by failing to implement adequate security systems, protocols and practices sufficient to protect the Financial Records and thereby creating a foreseeable risk of harm;

b. by failing to comply with the minimum industry data security standards;

c. by failing to timely and accurately discover and disclose to consumers that their Financial Records had been improperly accessed and acquired, and to adequately provide credit monitoring protection and other remediation and mitigation measures for Plaintiffs and the other Class members;

d. by retaining large amounts of sensitive information long after its legitimate business use was served.

61. In addition, Capital One voluntarily undertook duties to obtain, maintain, secure, and dispose of the Financial Records when it requested the information and retained the Financial Records for its own purposes. Its failure to employ reasonable and appropriate measures to safeguard and protect the Financial Records and in so doing prevent the Data Breach, constitutes a breach of this duty.

62. It was reasonably foreseeable to Capital One that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' personally identifiable information and Financial Records by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' personally identifiable information and Financial Records for no lawful purpose.

63. Capital One, by and through its above negligent or grossly negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' personally identifiable information and Financial Records within its possession, custody and control. Capital One, by and through its above negligent or grossly actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures, protocols, and software

and hardware systems for complying with the applicable laws and safeguarding and protecting their personally identifiable information and Financial Records.

64. But for Capital One's negligent or grossly negligent breach of the above-described duties owed to Plaintiffs and Class members, their personally identifiable information and Financial Records would not have been released, disclosed, and disseminated – without their authorization – and compromised.

65. Plaintiffs' and Class members' personally identifiable information and Financial Records was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Capital One's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class members' personally identifiable information and Financial Records.

66. As a direct and proximate result of Capital One's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, an imminent, immediate and continuing increased risk of improper disclosure, theft and misuse of their Financial Records, lost value of their Financial Records, and lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them – risks justifying expenditures for protective and remedial services for which they are entitled to compensation.

COUNT II
Negligence *Per Se*
(Brought by All Plaintiffs on Behalf of the Nationwide Class)

67. Plaintiffs incorporates paragraphs 1–54 as if fully set forth herein.

68. Defendant is a financial institution subject to the requirements of the Gramm-Leach-Bliley Act ("GLBA"). 15 U.S.C. § 6801.

69. Financial Records constitute nonpublic personal information, as defined by the GLBA. 15 U.S.C. § 6809.

70. Among other things, the GLBA requires companies to assess and address the risks to customer information in all areas of their operation. Rules promulgated under the GLBA require a written security plan reasonably designed to: (1) ensure the security and confidentiality of customer information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. 15 U.S.C. § 6801.

71. 16 C.F.R. §314.4 mandates the following requirements for financial institutions:

- Designate an employee or employees to coordinate your information security program.
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

    (1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

- Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

- Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

72. The written plan should be one that deters, detects, and defends against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively, including:

- Monitoring the websites of software vendors and reading relevant industry publications for news about emerging threats and available defenses.

- Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information.
- Check with software vendors regularly to get and install patches that resolve software vulnerabilities.
- Use anti-virus and anti-spyware software that updates automatically.
- Maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations.
- Regularly ensure that ports not used for your business are closed.
- Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.
- Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information.
- Use an up-to-date intrusion detection system to alert you of attacks.
- Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user.
- Insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.
- Take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet.
- Preserve and review files or programs that may reveal how the breach occurred.

- If feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.

73. Capital One's duties to use ordinary care in safeguarding Financial Records also arise from, *inter alia*, California's Financial Information Privacy Act (Cal. Fin. Code § 4050, *et seq*.), California's Customer Records Act (Cal. Civ. Code §§ 1798.80, *et seq*.), Article I, Section 1 of the California Constitution (California's constitutional right to privacy), California's UCL (Cal. Bus. & Prof. Code §§ 17200, *et seq*.), the Florida Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.201, *et seq*.), Tennessee's Financial Records Privacy Act (Tenn. Code § 45-10-101, *et seq*.), and Wisconsin's Trade Regulation For Disposal of Records Containing Personal Information (Wis. Stat. § 134.97).

74. Capital One violated these standards and duties by failing to adopt, implement, and maintain a written plan in compliance with the Safeguards Rule of the GLBA and above listed statutes with respect to Plaintiffs' and the Class members' Financial Records.

75. Plaintiffs and the other Class members are within the class of persons that the GLBA and above listed statutes are intended to protect, and the Financial Records contain the kind of information that are protected.

76. The harm that occurred as a result of the Data Breach is the type of harm the GLBA was designed to guard against. The Federal Trade Commission and other governmental authorities have pursued enforcement actions against businesses and financial institutions under similar circumstances.

77. As a direct and proximate result of Capital One's violation of the above laws, constituting negligence *per se*, Plaintiffs and the other Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach.

COUNT III
Breach of Confidentiality
(Brought by All Plaintiffs on Behalf of the Nationwide Class)

78. Plaintiffs incorporate paragraphs 1–54 as if fully set forth herein.

79. The Financial Records constitute private personally-identifiable information and financial information that is novel, unique, and confidential.

80. By entrusting their Financial Records to the care of Capital One, Plaintiffs and the other Class members entered into a relationship of trust and confidence that Capital One would employ reasonable and appropriate safeguards and procedures for storing, maintaining, and disposing the Financial Records.

81. Plaintiffs and the other Class members reasonably expected Capital One to take proper care of the Financial Records by observing reasonable and appropriate security measures, and not disclosing or sharing the information without authorization.

82. Capital One understood and Plaintiffs and the other Class members understood that the Financial Records were confidential information, provided to Capital One in confidence, and while Capital One retained the Financial Records, they would remain in confidence through the implementation and observance of reasonable and appropriate safeguards.

83. Capital One breached the confidentiality of the Financial Records in the Data Breach by disclosing the Financial Records to unauthorized, criminal actors who were able to access, view, and download the data from Capital One's systems.

84. Capital One breached the confidentiality of the Financial Records by failing to exercise reasonable care in maintaining, storing, and disposing of the Financial Records, which facilitated and led to the Data Breach and the failure to detect the Data Breach for an unreasonably long time.

85. As a direct and proximate result of Capital One's breach of confidence, Plaintiffs and the other Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach.

COUNT IV
Violation of California Customer Records Act,
California Civil Code §§ 1798.80, *et seq.* ("CRA")
(Brought by Plaintiff DeMarco on Behalf of the California Class)

86. Plaintiffs incorporate paragraphs 1–54 as if fully set forth herein.

87. For purposes of this Count IV, "Plaintiff" refers to Sean DeMarco.

88. Capital One is a "business" within the meaning of California Civil Code § 1798.80(a).

89. Plaintiff and each member of the California Class are "individuals" and "customers" within the meaning of California Civil Code § 1798.80(c) and (d).

90. California Civil Code § 1798.81 requires that businesses, such as Capital One, take all reasonable steps to dispose, or arrange for the disposal, of customer records within their custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means. Capital One retained Financial Records from 2005 through early 2019 and failed to take reasonable steps to dispose of these records when the legitimate business needs for them were served. Capital One had already rendered a decision as to the creditworthiness of Plaintiff and the other California Class members and therefore had no legitimate purpose for retaining the Financial Records. Had Capital One exercised reasonable care in disposing Financial Records, Plaintiff's and the other California Class members' personal information would not have been stolen.

91. California Civil Code § 1798.81.5 provides that a business that owns, licenses, or

maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

92. The Financial Records of Plaintiff and the other California Class members that was provided to Capital One constitute computerized data that includes Financial Records that is owned, licensed, or maintained by Capital One.

93. Capital One failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

94. Capital One's failure to have reasonable measures in place to secure the Financial Records was grossly negligent.

95. Capital One violated the Customer Records Act by failing to notify California residents in the most expedient time possible and without unreasonable delay. Capital One says it learned of the Data Breach by July 19, 2019, but reasonably should have discovered it much earlier. Upon learning of the Data Breach, it refused to notify a very large majority of the affected persons.

96. Furthermore, the notification was insufficient, misleading, and not compliant with the law. It unjustifiably downplays the risks caused by the Data Breach in a self-serving attempt to deny responsibility for the inevitable and well-documented costs of data breaches.

97. California law gives the protection of its citizens' privacy the highest priority. Article 1, Section 1 of the California Constitution states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursing and obtaining safety, happiness and privacy."

98. California's common law and statutory scheme also recognizes and protects California residents' right of privacy. For example, California Civil Code § 1798.81.5(a) states: It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information. California citizens' rights to privacy have been compromised and infringed by the acts and omissions of Capital One, as described herein.

99. Under § 1798.84 of the California Civil Code, any customer injured by a violation of this title may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.

100. As a result of Capital One's violation of the Customer Records Act and the Data Breach, Plaintiff and the other California Class members were injured and incurred actual harm and damages. Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Financial Records, lost value of their Financial Records, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT V
Violation of the Unfair Competition Act,
Business & Professions Code § 17200, *et seq.* ("UCL")
(Brought by Plaintiff DeMarco on Behalf of the California Class)

101. Plaintiffs incorporate paragraphs 1–54 as if fully set forth herein.

102. For purposes of this Count V, "Plaintiff" refers to Sean DeMarco.

103. Plaintiff brings this claim under the Unfair Competition Act (UCL), California Business & Professions Code § 17200, *et seq.*, on behalf of himself and the California Class.

104. California Business & Professions Code § 17200, *et seq.* provides that unfair

practices include, but are not limited to, "any unlawful, unfair or fraudulent business act[s] or practice[s]."

105. By and through its conduct, as described herein, Capital One engaged in activities that constitute unlawful, unfair and fraudulent business practices prohibited by California Business & Professions Code § 17200, *et seq.*

106. In the course of conducting its business, Capital One committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and the other California Class members' personally identifiable information and personal financial information, and violating the statutory and common law alleged herein in the process, including, *inter alia*, California's Financial Information Privacy Act (Cal. Fin. Code § 4050 *et seq.*), California's Customer Records Act (Cal. Civ. Code § 1798.80, *et seq.*), the Gramm-Leach Bliley Act (15 U.S.C. § 6801, *et seq.*), and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). Plaintiff and the other California Class members reserve the right to allege other violations of law by Capital One constituting other unlawful business acts or practices. Capital One's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

107. Capital One's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Capital One's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Capital One's practices are also contrary to legislatively declared

and public policies that seek to protect personally identifiable information and personal financial information and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as California's Financial Information Privacy Act (Cal. Fin. Code § 4050 *et seq.*), California's Customer Records Act (Civ. Code §§ 1798.80, *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, *et seq.*), and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). The gravity of Capital One's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Capital One's legitimate business interests other than engaging in the above-described wrongful conduct.

108. Capital One knew or should have known that failure to implement and maintain reasonable security procedures and practices to protect Plaintiff's and the other California Class members' Financial Records was unlawful, unfair, and fraudulent.

109. Capital One willfully ignored the clear and present risk of a data breach of its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the Data Breach.

110. Capital One retained Financial Records from 2005 through early 2019 and failed to take reasonable steps to dispose of these records when the legitimate business needs for them were served. Capital One had already rendered a decision as to the creditworthiness of Plaintiff and the other California Class members and therefore had no legitimate purpose for retaining the Financial Records. Had Capital One exercised reasonable care in disposing Financial Records, Plaintiff's and the other California Class members' personal information would not have been stolen.

111. The UCL also prohibits any "fraudulent business act or practice." Capital One's above-described claims, nondisclosures, and misleading statements were false, misleading and

likely to deceive the consuming public in violation of the UCL.

112. Capital One made misrepresentations on its website as alleged herein regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access. Moreover, Capital One's security measures were unable to detect any suspicious or unauthorized activity for a period of at least about four months, and perhaps longer.

113. Capital One benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

114. Capital One's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and the other California Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

115. Plaintiff and the other California Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff and the other California Class members largely had no idea that Capital One maintained their information at all, let alone had the negotiating power individually to demand adequate data security.

116. Capital One failed to provide timely, adequate, and reasonable notification to Plaintiff and the other California Class members. Capital One's press release unjustifiably downplays the risks caused by the Data Breach in a self-serving attempt to deny responsibility for the inevitable and well-documented costs of data breaches. Capital One also failed to provide adequate responses to inquiries by reducing visibility of the Data Breach, including from Internet browser searches.

117. As a direct and proximate result of Capital One's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the

Data Breach and their violations of the UCL, Plaintiffs and California Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia,*, identity theft, improper disclosure of their Financial Records, lost value of their Financial Records, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them – risks justifying expenditures for protective and remedial services for which they are entitled to compensation.

118. Unless restrained and enjoined, Capital One will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, California Class members, and the general public, also seeks restitution and an injunction prohibiting Capital One from continuing such wrongful conduct, and requiring Capital One to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the personally identifiable information and personal financial information entrusted to them, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

COUNT VI
Violation of The Florida Deceptive And Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq.* ("FDUTPA")
(Brought by Plaintiff Cox on Behalf of the Florida Class)

103. Plaintiffs incorporate paragraphs 1–54 as if fully set forth herein.

104. For purposes of this Count VI, "Plaintiff" refers to Samuel Cox.

105. Plaintiff and the other Florida Class members were subjected to Capital One's unconscionable and unfair and deceptive acts or practices, in violation of Fla. Stat. § 501.204, in

failing to properly implement adequate, commercially reasonable security measures to protect their Financial Records.

106. Capital One willfully ignored the clear and present risk of a data breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Data Breach.

107. Capital One benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

108. Capital One's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff Cox and the other Florida Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

109. Capital One retained Financial Records from 2005 through early 2019 and failed to take reasonable steps to dispose of these records when the legitimate business needs for them were served. Capital One had already rendered a decision as to the creditworthiness of Plaintiffs and the other Florida Class members and therefore had no legitimate purpose for retaining the Financial Records. Had Capital One exercised reasonable care in disposing Financial Records, Plaintiffs' and the other Florida Class members' personal information would not have been stolen.

110. Capital One's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

111. As a direct and proximate result of Capital One's wrongful conduct, Plaintiff Cox and the other Florida Class members have suffered actual damages including improper disclosure of their Financial Records, lost value of their Financial Records, lost time and money incurred to

mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

112. Plaintiff Cox's and the other Florida Class members' injuries were proximately caused by Capital One's violations of the Florida Deceptive and Unfair Trade Practices Act.

COUNT VII
Violation of Tennessee Financial Records Privacy Act
Tenn. Code §§ 45-10-101, *et seq.* (TFRPA")
(Brought by Plaintiffs Greer and Yoder on Behalf of the Tennessee Class)

113. Plaintiffs incorporate paragraphs 1–54 as if fully set forth herein.

114. For purposes of this Count VII, "Plaintiffs" refers to Nicole Greer and Jason Yoder.

115. The Tennessee Financial Records Privacy Act makes it illegal for a financial institution to disclose financial records of a customer to any person other than the customer or the customer's agent. Tenn. Code § 45-10-104.

116. Plaintiffs and the other members of the Tennessee class were subjected to Capital One's unauthorized disclosure of their Financial Records, in violation of Tennessee Code § 45-10-104, in failing to properly implement adequate, commercially reasonable security measures to protect their Financial Records and preventing disclosure to unauthorized persons.

117. Capital One willfully ignored the clear and present risk of a data breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Data Breach.

118. Capital One benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

119. Capital One's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiffs and the other Tennessee Class

members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

120. Capital One retained Financial Records from 2005 through early 2019 and failed to take reasonable steps to dispose of these records when the legitimate business needs for them were served. Capital One had already rendered a decision as to the creditworthiness of Plaintiffs and the other Tennessee Class members and therefore had no legitimate purpose for retaining the Financial Records. Had Capital One exercised reasonable care in disposing Financial Records, Plaintiffs' and the other Tennessee Class members' personal information would not have been stolen.

121. Capital One's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

122. As a direct and proximate result of Capital One's wrongful conduct, Plaintiffs and the other Tennessee Class members have suffered actual damages including improper disclosure of their Financial Records, lost value of their Financial Records, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

123. Plaintiffs and the other Tennessee Class members' injuries were proximately caused by Capital One's violations of the Tennessee Financial Records Privacy Act.

COUNT VIII
Violation of Wisconsin Trade Regulation For Disposal of Records Containing Personal Information Wis. Stat. § 134.97
(Brought by Plaintiff Leffler on Behalf of the Wisconsin Class)

124. Plaintiffs incorporate paragraphs 1–54 as if fully set forth herein.

125. For purposes of this Count VIII, "Plaintiff" refers to Thomas Leffler.

126. Capital One is a financial institution as defined in Wis. Stat. § 134.97.

127. Plaintiff's and the other Wisconsin Class members' Financial Records constitute "personal information" as defined by Wis. Stat. § 134.97.

128. Capital One failed to properly dispose of Plaintiff's and the other Wisconsin Class members' Financial Records and failed to take actions reasonably ensuring that no unauthorized person will have access to the Financial Records in violation of Wis. Stat. § 134.97, in failing to properly maintain reasonable security over the systems where the Financial Records were kept and facilitating the Data Breach. As set forth herein, Capital One failed in its obligations to dispose properly of the Financial Records by placing them on an unsecured computer system, capable of being accessed from unauthorized outside persons, capable of being unencrypted or not encrypted at all, and all without being detected. In addition, Capital One should have timely disposed of Financial Records and not retained them indefinitely as it apparently did.

129. As a direct and proximate result of Capital One's wrongful conduct, Plaintiff and the other Wisconsin Class members have suffered actual damages, including identity theft, improper disclosure of their Financial Records, lost value of their Financial Records, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT IX
Unjust Enrichment
(Brought By All Plaintiffs On Behalf of the Nationwide Class)

130. Plaintiffs incorporate paragraphs 1–54 as if fully set forth herein.

131. Plaintiffs and the other Class members conferred a monetary benefit on Capital One. Specifically, Plaintiffs and the other Class members paid for services provided by Capital One and provided Capital One with Financial Records or authorization to access such information in determining eligibility for credit. In exchange, Plaintiffs and the other Class members were

entitled to have Capital One protect and securely maintain their Financial Records and safely dispose of the information when Capital One no longer had legitimate business use for it.

132. Capital One knew that Plaintiffs and the other Class members conferred a benefit on Capital One. Capital One profited from the Plaintiffs' and the other Class members' use of its services and from unreasonably, wrongfully, and inequitably diverting funds that should have been allocated toward reasonably adequate security toward other profit-driven goals of Capital One's business.

133. Capital One failed to secure Plaintiffs' and the other Class members' Financial Records and therefore did not provide the full compensation for the benefit the Plaintiffs and the other Class members conferred. Capital One inequitably acquired profits from the funds it wrongfully diverted from providing reasonable security toward other money making endeavors at the expense of Plaintiffs and the Class members.

134. Under the circumstances, it would be unjust for Capital One to be permitted to retain the benefits of its unlawful conduct. Capital One should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and the other Class members proceeds that it unjustly received from its unconscionable and inequitable conduct.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this complaint so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. Certifying the Classes as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Ordering Defendant to pay actual damages to Plaintiffs and the other members of the Classes;

C. Ordering Defendant to pay statutory damages to Plaintiffs and the other members of the Classes;

D. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Classes;

E. Ordering Defendant to pay restitution and disgorgement, and injunctive and declaratory relief, and other equitable relief;

F. Imposing on Defendant a constructive trust or common fund for the benefit of Plaintiffs and the other members of the Classes;

F. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiffs;

G. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded as allowable by law; and

H. Ordering such other and further relief as may be just and proper.

Date: August 8, 2019

Respectfully Submitted,

/s/ Grant Morris

Grant Morris (Va. Bar No. 16290)
SANFORD HEISLER SHARP, LLP
700 Pennsylvania Avenue SE, Suite 300
Washington, DC 20003
Tel: (646) 402-5650
gmorris@sanfordheisler.com

Kevin Sharp (pro hac vice to be filed)
SANFORD HEISLER SHARP, LLP
611 Commerce Street, Suite 3100
Nashville, TN 37203
Tel: 615-434-7000
ksharp@sanfordheisler.com

Adán Martínez (pro hac vice to be filed)
SANFORD HEISLER SHARP, LLP
1350 Avenue of the Americas, 31st Floor
New York, NY 10019
Tel: (646) 402-5650
amartinez@sanfordheisler.com

Ben Barnow (pro hac vice to be filed)
Erich P. Schork (pro hac vice to be filed)
Jeffrey D. Blake (pro hac vice to be filed)
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
j.blake@barnowlaw.com

Timothy G. Blood (pro hac vice to be filed)
Thomas J. O'Reardon, II
BLOOD HURST & O'REARDON, LLP
701 B Street, Suite 1700
San Diego, CA 92101
Tel: (619) 338-1100
tblood@bholaw.com
toreardon@bholaw.com

Shpetim Ademi (pro hac vice to be filed)
Ben J. Slatky (pro hac vice to be filed)
ADEMI & O'REILLY, LLP
3620 East Layton Avenue
Cudahy, WI 53110
Tel: (414) 482-8000
sademi@ademilaw.com
bslatky@ademilaw.com

Plaintiffs' Counsel